Job Description – Solution Architect

The Solution Architect – Cybersecurity is responsible for designing, implementing, and overseeing secure technology solutions that align with the organization's strategic objectives. This role combines deep technical expertise with a strong understanding of business processes to ensure the security architecture supports both innovation and compliance.

Key Responsibilities

1. Solution Design & Architecture

- Develop and document end-to-end cybersecurity architectures and blueprints for enterprise systems, applications, and infrastructure.
- Ensure proposed solutions meet security, regulatory, and business requirements.
- Integrate cybersecurity controls into cloud, network, application, and data platforms.
- Evaluate and recommend security technologies, tools, and vendors

2. Security Strategy & Governance

- Contribute to the organization's cybersecurity strategy, frameworks, and policies.
- Ensure alignment with standards such as ISO 27001, NIST, CIS, and relevant industry regulations (e.g., GDPR, PCI DSS).
- Collaborate with enterprise architects to ensure security-by-design principles are embedded into all IT initiatives.

3. Technical Leadership

- Lead security architecture reviews and threat modeling exercises.
- Provide subject matter expertise during project planning, solution design, and implementation phases.
- Guide development and operations teams on secure coding, configuration, and deployment practices (e.g., DevSecOps).

4. Risk Management

- Identify, assess, and mitigate security risks in proposed and existing solutions.

- Support incident response and post-incident analysis to improve architectural resilience.

5. Stakeholder Engagement

- Collaborate with IT, engineering, compliance, and business stakeholders to translate business needs into secure solutions.
- Present architecture decisions and risk assessments to senior management and governance boards.

Required Qualifications

- Bachelor's degree in computer science, Information Security, or related field (master's preferred).
- 7+ years of experience in IT, with at least 3–5 years in a security architecture or senior cybersecurity engineering role.
- Proven experience designing secure solutions in **cloud (AWS, Azure, GCP)** and **on-premises** environments.
- Strong understanding of **network security, identity & access management (IAM), encryption, endpoint protection, SIEM, and zero-trust architecture**.
- Familiarity with **DevSecOps**, container security (Docker, Kubernetes), and API security.

Certifications (Preferred)

- **CISSP** – Certified Information Systems Security Professional
- **CCSP** – Certified Cloud Security Professional
- **SABSA** / **TOGAF** – Enterprise or Solution Architecture Framework
- **CISM**, **CEH**, or vendor-specific cloud security certifications (e.g., AWS Certified Security, Azure Security Engineer Associate)